## AMENDMENTS TO THE SPECIFICATION

Please replace the paragraph at page 8, lines 3-14 with the following amended paragraph:

The network-based firewall 102 includes the network interface 134, firewall process 136 including computing processing (not shown) such as processor, system interfaces, local interfaces, among others, memory 138, a protected ~~network 142~~ network 103, such as an intranet, and a network interface 144 for communicating with the provider network 104. The software and/or firmware in memory 138 may include one or more separate programs, each of which comprises an ordered listing of executable instructions for implementing logical functions. In the example of FIG. 1, the software in the memory 138 can include a policy modification agent (PMA) logic 140, and a suitable operating system (O/S) 139. The operating system 139 preferably controls the execution of other computer programs, and provides scheduling, input-output control, file and data management, memory management, and communication control and related services, among others.

Please replace the paragraph at page 10, line 19 through page 11, line 7 with the following amended paragraph:

Upon receipt of a positive acknowledgement sent to the FFC 108 from the PMA 140 indicating that the time window is acceptable to the firewall, the FFC 108 sends an acknowledgement back to the user's processing device 110 via, for example the secure transceiver 202 communicating to the host computer 106. This acknowledgement preferably includes the time window information, among other information. If a negative acknowledgement is received from the PMA 140, the FFC controller 204 may instruct the firewall policy configuration/modification window generator 210 of the FFC 108 to calculate another time window and try again. Optionally, the FFC 108 may keep a record of ~~previously times~~ previous time window requests sent to the PMA 140 that have been positively acknowledged, so that it can use this record to avoid making any future time window requests for time windows that are already scheduled in the PMA 140 and therefore will not be available. In a preferred embodiment, if a configurable number of successive time windows are attempted by

the FFC 108 with only negative acknowledgments being received from the PMA 140, the FFC 108 may then send a "failed" acknowledgement to the user's processing device 110 and notify others, such as administrators or help desk staff as appropriate via standard methods such as email, pager alerts, or various alarms, and optionally indicate in the "failed" user acknowledgement that the user or customer should request assistance. In an alternative preferred embodiment, the FFC 108 asks the user via the user's processing device 110 if the user wishes to continue the repetitive time window generation attempts until satisfactory results are obtained, or until optional additional configurable limits are exceeded.

Please replace the paragraph at page 12, line 32 through page 13, line 28 with the following amended paragraph:

FIG. 3 is a block diagram depicting a preferred embodiment of a policy modification agent (PMA) 140 of a system for network firewall policy configuration facilitation. In a preferred embodiment the PMA 140 resides on (or is attached to) the network-based firewall 102 and is adapted to receive communications from the FFC 108. In addition, the PMA 140 is configured to communicate with and influence the firewall process 136 that include a security policy encompassing a set of filtering rules. In a preferred embodiment, the PMA 140 includes a number of modules, such as a secure transceiver 302, PMA controller 304, policy modifier 306, blocking history checker 308, and blocking database 310. The secure transceiver 302 is responsible for adding encryption and authentication to communications transmitted from the PMA 140, and for authenticating and decrypting communications received by the PMA 140. The PMA controller 304 provides overall control functionality to the PMA 140, for instance coordinating the actions of the various modules, providing time window packet observations to the blocking history checker 308, and providing information to the policy modifier 306 regarding policy change requirements. The policy modifier 306 modifies the firewall policy 312, and also communicates the observations of the firewall packet inspector 314 to the PMA controller 304 during the time window. The blocking history checker 308 uses time window packet observations from the PMA controller to check the blocking history database 310 for previously observed packets, previous policy modification attempts and results, etc. The blocking database 310 can be used to record any desired information helpful to the policy modification process,

including for instance previously observed packets associated with a particular host, previously observed packets associated with a particular application, packets observed during particular time windows, results of previous attempts to modify the firewall policy associated with particular hosts and/or applications, etc. In an example, these modules are software process, modules or routines. In an alternative embodiment, the modules can be partly or fully implemented in hardware. The PMA 140 preferably utilizes existing firewall process 136 components or modules, which typically includes some form or arrangement of firewall policy 312, firewall packet inspector 314, and firewall ~~filter 318~~ filter 316.

Please replace the paragraph at page 13, line 39 through page 14, line 25 with the following amended paragraph:

In an example, the secure transceiver 302 via the network interface 134 receives a time window request for a particular user and application from the FFC 108 in order to add a new application to the user's/customer's firewall policy as described above, the PMA controller 304 checks to see if the time window is available, and if available the PMA controller 304 sends an acknowledgement to the FCC 108 and likewise schedules the time window. If the time window is unavailable, the PMA 140 sends this information to the FFC 108 so that the FFC 108 can request a different time window. The PMA 140 may optionally include information on currently available time periods so as to aid the FFC 108 in selecting another time window, in which case the FFC 108 may then optionally keep a record of this information so that it can consult this record when sending future time window requests to the PMA, 140 in order to select or generate time windows which are likely to be currently unscheduled and thus acceptable to the PMA 140. For example, the secure transceiver 302 via the network interface 134 is in communication with the FFC 108 to send and receive messages containing the above-mentioned information and acknowledgements to/from the FFC 108. Information from the secure transceiver 302 is communicated to the PMA controller 304. The PMA controller 304 communicates with both the policy modifier 306 and the blocking history checker 308. When the time of a scheduled time window arrives, the PMA controller 304 communicates this to the policy ~~modifier 304~~ modifier 306, which communicates with the firewall packet inspector 314 to observe the packets flowing through the firewall associated with the user/customer, presuming that these should be associated

with the new application being exercised at that time. The blocking history checker 308 provides the PMA controller 304 access to the blocking database 310 that includes information on questionable packets associated with that user/customer and information regarding any previous policy modification attempts for the new application. The policy modifier 306 also communicates with the firewall policy 312 for the purpose of modifying the policy filtering rules as needed, and for negotiating the manner in which these rules can be modified (which may be dependent upon the particular firewall brand, model, and implementation).